

REMARKS

Claims 38, 49, 60 and 73 have been amended.

Claims 38-63, 65-76, 78-85 and 88 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (US Patent 6,163,771) ("Walker") in view of Brake Jr. et al. (US Patent 7,072,864) ("Brake") and further in view Curry et al. (US Patent 5,949,880) ("Curry"). Independent claims 38, 49, 60 and 73 have been amended and with respect to these claims, and their dependent claims, the Examiner's rejection is respectfully traversed.

Independent claim 38 has been amended to recite the initial step of "generating by a financial institution a funds-access code" including the steps of "generating by a computer a random code that is the funds-access code," and "creating and storing a funds access code record containing the generated funds-access code and accompanying identification information about a recipient in a database accessible to a computer connected to a communication network."

Furthermore, independent claim 38 has been amended to recite the subsequent step of "validating by the distributor the presented funds-access code" including the steps of "accessing the funds-access code record on the database via a remote computer connected to the communication network" and "comparing the presented funds-access code and the presented recipient identification information with the funds-access code and the recipient identification information stored in the funds access code record." Independent claims 49, 60 and 73 have been amended to recite similar features.

The method recited in amended claim 38 is not taught or suggested in the cited prior art. In the Office Action, the Examiner argues that Walker discloses "generating a funds-access code (Abstract) including the steps of creating and storing a record containing the generated funds-

access code and *accompanying information about a recipient* in a database on a computer readable medium accessible to a computer connected to a communication network, (column 7, lines 20-45) and linking the record containing the funds-access code to a financial instrument containing funds; (Figure 6, private key and nonce in relation to account number)” (page 3, lines 8-13).

Also, the Examiner acknowledged that Walker does not explicitly disclose “generating by a computer a random code that is the funds-access code; validating the presented funds-access code including the steps of transmitting by the distributor the presented funds-access code and recipient information via a remote computer connected to the communication network” (page 4, lines 19-22). However, the Examiner argues that Curry discloses “generating by a computer a random code that is the funds-access code; (column 6, lines 6-30; column 7, lines 27-54 [examiner notes that the Random SALT value added to the transaction block data effectively randomize the data])” and “validating the presented funds-access code including the steps of transmitting by the distributor the presented funds-access code and recipient information via a remote computer connected to the communication network (column 7, lines 14-37)” (page 5, lines 3-9).

Applicant has reviewed Walker and Curry and applicant does not believe these references disclose generating by a financial institution a funds-access code including the steps of generating by a computer a random code that is the funds-access code, creating and storing a funds access code record containing the generated funds-access code and accompanying identification information about a recipient in a database accessible to a computer connected to a communication network and linking the funds access code record to a financial instrument

containing funds and validating by the distributor the presented funds-access code” including the steps of accessing the funds-access code record on the database via a remote computer connected to the communication network and comparing the presented funds-access code and the presented recipient identification information with the funds-access code and the recipient identification information stored in the funds access code record as recited in amended independent claim 38.

Specifically, Walker, as shown in Fig. 3, discloses a cardholder initiating a transaction by generating a single-use number 300 using a credit card. The generated single-use number 300 is provided to a merchant who enters the number into an authorized terminal connected to a central credit card processing system 303 maintained by the issuer of the credit card (col. 6, lines 39-43). The central credit card processing system 303 determines whether or not the single-use number is valid (col. 6, lines 46-49). If valid, the central credit card processing system 303 returns an authorization code 310 to the merchant and the merchant 302 provides the cardholder 301 with goods or services 320 (col. 6, lines 49-53).

As shown in Fig. 4, the central credit card processing system 303 includes a storage device 410 containing a credit card account holder database 411, a credit card account private key database 412 and a credit card transaction database 413 (col. 5, lines 9-19).

The credit card account holder database 411 tracks all cardholder accounts. As shown in Fig. 5, each record of this database includes a cardholder account number 501, a cardholder's name 502, address 503, and telephone number 504, an original credit line 505 associated with a account, an amount of credit currently available 506 and an expiration date 507 (col. 7, lines 20-26).

The credit card account private key database 412 contains constants for each cardholder account number used to generate the single-use number. As shown in Fig. 6, each record of this database includes a cardholder private key 601, a cardholder account number 501 and a nonce number 602 (col. 7, lines 27-36). Along with these constants, the credit card uses an initialization variable that is incremented with each transaction.

The credit card transaction database 413 contains a listing of each authorized transaction. As shown in Fig. 7, each record of this database includes the account number 501, the expiration date of the card 507, the transaction amount 702, the merchant identification number 703 and an initialization number 704 (col. 7, lines 37-45).

To validate the single-use number, the central credit card processing system 303 first extracts the encrypted nonce, the initialization variable and the account number from the single-use number (col. 8, lines 40-44). The processor then retrieves the extracted account number from the cardholder account database 411 and determines whether the account number is valid (col. 8, lines 44-47). If the account number is valid, the processor looks up the initialization variable in the credit card transaction database 413 to determine whether the cardholder has previously used the initialization variable (col. 8, lines 47-51). If the initialization variable has not been used, the it is stored in the credit card transactional database 413 (col. 8, lines 52-55). Lastly, the processor retrieves the card holder's private key from the private key database 412 and uses it to decrypt the encrypted nonce (col. 8, lines 56-58). The decrypted nonce is compared to the nonce stored in the account private key database 412 (col. 8, lines 62-63). If they match, the single-use number is considered valid (col. 8, lines 63-65).

Therefore, Walker discloses generating a single-use number on a credit card using a cardholder private key, a cardholder account number and a nonce number that are stored on the credit card and an initialization number that is incremented with each transaction and then providing the generated single-use number to a merchant. However, Walker does not disclose specifying a merchant and saving the identification information of the specified merchant while generating the single-use number and prior to providing the generated single-use number to a merchant. Rather, Walker discloses only that a merchant's identification number in a transactional database after the issuer of the credit card has received a single-use number from the merchant and has validated that single-use number.

Furthermore, Walker discloses the card issuer validating a single-use number received from a merchant by extracting the encrypted nonce, the initialization variable and the account number from the received single-use number, accessing the cardholder account database to validate the extracted account number, accessing the credit card transaction database to validate the extracted initialization variable and accessing the account private key database to validate the extracted nonce. However, Walker does not disclose extracting information as to the identity of an intended merchant from the received single-use number and accessing a database to confirm the validity of the merchant identity information as a prerequisite to validating the received single-use number.

Moreover, Curry does not disclose anything that would change this conclusion. Curry, as shown in Fig. 4, discloses validating encrypted valuable information transferred from a portable module to a secure module within a microprocessor based device. When the portable module is put in contact with the microprocessor based device, the microprocessor based device reads X2

a portable module's ID number, a transaction count and an encrypted data packet from a memory within the portable device X1 (col. 7, lines 37-39). Encrypted within the data packet is a portable module ID number, a portable module transaction count number and an amount of value (the monetary value) of the portable module at the present time (col. 7, lines 23-27). The secure module decrypts the encrypted data packet using a public key X4 (col. 7, lines 47-49). The secure module compares the serial number received from the portable module with the decrypted serial number X5 (col. 7, lines 43-44). If the two serial numbers match, the secure module then compares the transaction count received from the portable module with the decrypted transaction count X6 (col. 7, lines 49-51). If the two transaction counts also match then the secure module is comfortable that the data received from the portable module is not counterfeit X7 (col. 7, lines 51-53). Furthermore, a time stamp may have been sent from the portable device which is then used by the secure device to determine whether the portable module is still valid (col. 7, lines 55-60).

Therefore, Curry discloses a portable module transferring a portable module's ID number, a transaction count and an encrypted data packet to a secure module within a microprocessor device, the encrypted data packet including a portable module ID number, a portable module transaction count number and an amount of value (the monetary value) of the portable module at the present time. However, Curry does not disclose the portable module specifying a merchant for a specific transaction and then transferring identification information of that specified merchant to the secure module along with a portable module's ID number, a transaction count and an encrypted data packet to a secure module within a microprocessor device.

Furthermore, Curry discloses validating the data received from the portable module by comparing the received portable module's ID number and transaction count with the decrypted portable module ID and transaction count and determining whether the portable module is still valid based on a time stamp also received from the portable module. However, Curry does not disclose the secure module comparing a merchant identification information received from the portable module with an encrypted identification information in order to validate the data received from portable module or for validating a transaction between the portable module and the microprocessor device.


Moreover, Brake does not disclose anything that would change these conclusions.

Accordingly, the combination of Walker, Brake and Curry does not teach or suggest generating by a financial institution a funds-access code including the steps of generating by a computer a random code that is the funds-access code, creating and storing a funds access code record containing the generated funds-access code and accompanying identification information about a recipient in a database accessible to a computer connected to a communication network and linking the funds access code record to a financial instrument containing funds and validating by the distributor the presented funds-access code" including the steps of accessing the funds-access code record on the database via a remote computer connected to the communication network and comparing the presented funds-access code and the presented recipient identification information with the funds-access code and the recipient identification information stored in the funds access code record as recited in amended independent claims 38, 49, 60 and 73.

Accordingly, it is requested that the rejections of claims 38, 49, 60 and 73 and the dependent claims under 35 U.S.C. 103 be withdrawn.

In light of the foregoing, reconsideration and allowance of this application are respectfully requested.

Respectfully submitted,

By: 
Mark Montague
Reg. No. 36,612
Attorney of Record

COWAN, LIEBOWITZ & LATMAN, P.C
1133 Avenue of the Americas
New York, New York 10036-6799
(212) 790-9200